Indistinguishability and semantic security for quantum encryption scheme

Chong Xiang[a], Li Yang[a,*]

[a] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*

Abstract

We investigate the definition of security for encryption scheme in quantum context. We systematically define the indistinguishability and semantic security for quantum public-key and private-key encryption schemes, and for computational security, physical security and information-theoretic security. Based on our definition, we present a necessary and sufficient condition that leads to information-theoretic indistinguishability for quantum encryption scheme. The equivalence between the indistinguishability and semantic security of quantum encryption scheme is also proved.

Keywords: indistinguishability, semantic security, quantum encryption scheme

1. Introduction

The definition of security for encryption scheme is an important area of cryptography. Up till now, both the quantum public-key encryption [1, 2, 3, 4, 5] and quantum private-key encryption [6, 7, 8] has been carried out. Here we investigate the indistinguishability and semantic security into quantum context which would be useful for analysis the security of quantum encryption schemes.

In our previous work, we have already shown the definition of the indistinguishability for quantum public-key encryption scheme[9], for quantum private-key encryption scheme[10],and for quantum bit commitment scheme and have presented a necessary and sufficient condition leads to

*Corresponding author. E-mail: yangli@iie.ac.cn

this security[11]. Here we will systematically define the indistinguishability and semantic security for quantum public-key and private-key encryption schemes, and for computational security, physical security and information-theoretic security.

The quantum parameters are continuous variable. In order to give the definition of indistinguishability for quantum encryption scheme, we first give a definition of indistinguishability for encryption scheme with continuous variable based on probability density function, and a definition of indistinguishability based on multi-circuits. We show that these definitions are equivalent. Then we prove that the indistinguishability based on multi-circuits is equivalent to ordinary indistinguishability with single-circuit. Then we get the definition of indistinguishability for quantum encryption scheme. Similarly we define the semantic security.

The equivalence between computational indistinguishability and semantic security for classical encryption scheme is already proved, but the equivalence for information-theoretic ones is still an open problem. For public-key encryption scheme, there is no information-theoretically secure classical public-key encryption scheme, so we discuss the equivalence between computational indistinguishability and semantic security for quantum encryption scheme and between information-theoretic ones. About private-key encryption scheme, the equivalence between computational indistinguishability and semantic security for quantum encryption scheme and between information-theoretic ones for classical and quantum encryption schemes all are discussed.

2. Preliminaries

The definitions of indistinguishability and semantic security were firstly presented by S. Goldwasser and S. Milcali[12, 13], then Goldrich[14] developed these definitions and classify defined the indistinguishability and semantic security with different conditions.

2.1. Indistinguishability

The indistinguishability for private-key encryption scheme is:

Definition 1. (indistinguishability for private-key encryption scheme): *A private-key encryption scheme, (G, E, D), is said to be an indistinguishable scheme if for every polynomial-size circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and every $x, y \in \{0,1\}^{Poly(n)}$,*

$$|\Pr[C_n(E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(E_{G_1(1^n)}(y)) = 1]| < \frac{1}{p(n)}. \quad (1)$$

For public-key encryption scheme, the indistinguishability is defined as:

Definition 2. (indistinguishability for public-key encryption scheme): *A public-key encryption scheme, (G, E, D), is said to be an indistinguishable scheme if for every polynomial-size circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and every $x, y \in \{0,1\}^{Poly(n)}$,*

$$|\Pr[C_n(G_1(1^n), E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(G_1(1^n), E_{G_1(1^n)}(y)) = 1]| < \frac{1}{p(n)}. \quad (2)$$

These definitions are based on computational security, if the inequalities are satisfied for every circuit family $\{C_n\}$ instead of for every polynomial-size circuit family $\{C_n\}$, we gains the definitions based on information-theoretic security.

2.2. Semantic security

The semantic security for private-key encryption scheme is shown as:

Definition 3. (semantic security for private-key encryption scheme):

A private-key encryption scheme, (G, E, D), is said to be semantically secure if for every probabilistic polynomial-time algorithm A there exists a probabilistic polynomial-time algorithm A' such that for every probability ensemble $\{X_n\}_{n\in\mathbb{N}}$, with $|X_n| \le poly(n)$, every pair of polynomially bounded functions $f(\cdot), h(\cdot)$: $\{0,1\}^* \to \{0,1\}^*$, every positive polynomial $p(\cdot)$ and all sufficiently large n,

$$\begin{aligned} & \Pr[A(1^n, E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\ < \; & \Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n) + \frac{1}{p(n)}. \end{aligned} \quad (3)$$

For public-key encryption scheme, it is:

Definition 4. (indistinguishability for public-key encryption scheme):

A public-key encryption scheme, (G, E, D), is said to be semantically secure if for every probabilistic polynomial-time algorithm A there exists a probabilistic polynomial-time algorithm A' such that for every $\{X_n\}_{n\in\mathbb{N}}, f(\cdot), h(\cdot) p(\cdot)$ and n as in Definition 3,

$$
\begin{aligned}
& \Pr[A(1^n, G_1(1^n), E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\
< \; & \Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) \\
= \; & f(1^n, X_n) + \frac{1}{p(n)}.
\end{aligned} \tag{4}
$$

Similarly, These definitions are based on computational security, if the inequalities are satisfied that for every algorithm A there exists a probabilistic algorithm A' instead of for every polynomial-time algorithm A there exists a probabilistic polynomial-time algorithm A', we gains the definitions based on information-theoretic security.

3. Indistinguishability for quantum encryption scheme

Firstly, we discuss the indistinguishability of quantum private-key encryption scheme based on that of classical private-key encryption scheme.

3.1. Indistinguishability based on probability density function

As the quantum information is continuous character, if we want to define the indistinguishability of quantum encryption scheme, firstly we should present the indistinguishability of continuous variable. It must depend on the probability density function, so we give the C-indistinguishability of classical information as follow:

Definition 5. *If the plaintext is continuous variable, let the probability density function of plaintext space P is $q(x)$, which is a continuous function. A private-key encryption scheme, (G, E, D), is said to be a C-indistinguishable scheme if it satisfies the condition as follow: for every polynomial-size circuit families $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and every $x, y \in P$,*

$$
\left|\Pr[C_n(E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(E_{G_1(1^n)}(y)) = 1]\right| < \frac{1}{p(n)}. \tag{5}
$$

3.2. Indistinguishability based on multi-circuits

Then we show a definition of indistinguishability based on multi-circuits as follow:

Definition 6. *A private-key encryption scheme, (G, E, D), is said to be a M-indistinguishable scheme if for every polynomial-size circuit families $\{C_n^i\}$, here $i = 1, 2 \cdots, m$, every positive polynomial $p_i(\cdot)$, all sufficiently large n, and every $x_i, y_i \in \{0,1\}^{Poly(n)}$,*

$$\begin{aligned}
|\Pr[C_n^1(E_{G_1(1^n)}(x_1)) = 1] &- \Pr[C_n^1(E_{G_1(1^n)}(y_1)) = 1]| < \frac{1}{p_1(n)}, \\
|\Pr[C_n^2(E_{G_1(1^n)}(x_2)) = 1] &- \Pr[C_n^2(E_{G_1(1^n)}(y_2)) = 1]| < \frac{1}{p_2(n)}, \\
&\vdots \\
|\Pr[C_n^m(E_{G_1(1^n)}(x_m)) = 1] &- \Pr[C_n^m(E_{G_1(1^n)}(y_m)) = 1]| < \frac{1}{p_m(n)}. \quad (6)
\end{aligned}$$

3.3. Equivalence of the definitions

Based on above definitions of indistinguishability, we will prove that they are all equivalence. The proofs in this section are all based on definitions of computational security.

Lemma 1. *If a private-key encryption scheme is said to be a M-indistinguishable scheme if and only if it is an indistinguishable scheme.*

Proof. For both sufficiency and necessity, we can prove with reduction to absurdity. Here we prove the sufficiency for example:

If the scheme is not M-indistinguishable, there must exist at least a polynomial-size circuit family $\{C_n^i\}$, a positive polynomial $p_i(\cdot)$, and $x_i, y_i \in \{0,1\}^{Poly(n)}$, which lead to that for all sufficiently large n

$$|\Pr[C_n^i(E_{G_1(1^n)}(x_i)) = 1] - \Pr[C_n^i(E_{G_1(1^n)}(y_i)) = 1]| \geq \frac{1}{p_i(n)}. \quad (7)$$

Therefore, if we let $\{C_n\} = \{C_n^i\}$, $p(\cdot) = p_i(\cdot)$, $x = x_i, y = y_i$, we can get:

$$|\Pr[C_n(E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(E_{G_1(1^n)}(y)) = 1]| \geq \frac{1}{p(n)}, \quad (8)$$

for all sufficiently large n, which means this scheme is not indistinguishable.

Thus the sufficiency is proved.

Similarly, we can use prove the necessity. □

Lemma 2. *If a private-key encryption scheme with continuous plaintext is said to be a C-indistinguishable scheme if it is a indistinguishable scheme.*

Proof. Assume the scheme is not a C-indistinguishable scheme, there must exist $x, y \in P$, which satisfy that for all sufficiently large n, every polynomial-size circuit families $\{C_n\}$, every positive polynomial $p(\cdot)$:

$$\left|\Pr[C_n(E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(E_{G_1(1^n)}(y)) = 1]\right| \geq \frac{1}{p(n)}. \tag{9}$$

Let $n_0 = max\{|x|, |y|\}$, here $|x|$ is the length of x, and let $n > n_0$, we can get that: there exist $x, y \in \{0,1\}^{Poly(n)}$, which satisfy that for all sufficiently large n, every polynomial-size circuit families $\{C_n\}$, every positive polynomial $p(\cdot)$:

$$\left|\Pr[C_n(E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(E_{G_1(1^n)}(y)) = 1]\right| \geq \frac{1}{p(n)}. \tag{10}$$

This reaches a contradiction to the hypothesis that the scheme is a indistinguishable scheme. Thus the lemma follows. □

The equivalence of these definitions is almost proved except the necessity of lemma.2, we planed to complete this side via the definition based on multi-circuits, but it has not worked out yet, so it is still a conjecture.

Conjecture 1. *If a private-key encryption scheme with continuous plaintext is said to be a C-indistinguishable scheme if and only if it is a M-indistinguishable scheme.*

3.4. Indistinguishability for quantum encryption scheme

As the indistinguishability of classical private-key encryption scheme can lead to that of continuous variable, We suggest here a definition of information-theoretic indistinguishability for quantum private-key encryption scheme as follow:

Definition 7. *A quantum private-key encryption scheme is information-theoretically indistinguishable if for every quantum circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n's, and every $x, y \in \{0,1\}$:*

$$\left|\Pr[C_n(E_{G(1^n)}(x)) = 1] - \Pr[C_n(E_{G(1^n)}(y)) = 1]\right| < \frac{1}{p(n)}, \tag{11}$$

where the encryption algorithm E should be a quantum algorithm, and the ciphertext $E(x), E(y)$ are quantum states.

Similarly, for quantum public-key encryption scheme, the information-theoretic indistinguishability is shown as:

Definition 8. *A quantum public-key encryption scheme is information-theoretically indistinguishable if for every quantum circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n's, and every x, y in plaintext space:*

$$\left|\Pr[C_n(G(1^n), E_{G(1^n)}(x) = 1] - \Pr[C_n(G(1^n), E_{G(1^n)}(y) = 1]\right| < \frac{1}{p(n)}, \quad (12)$$

where the encryption algorithm E should be a quantum algorithm, and the ciphertext $E(x), E(y)$ are quantum states.

In classical context, the security is defined under two conditions, here the quantum definitions can be classified by three different conditions:

1. As defined above, we get the definitions of information-theoretic indistinguishability.
2. If the inequalities are satisfied for polynomial-size quantum circuit family $\{C_n\}$ instead of for every circuit family $\{C_n\}$, it results the definitions of computational indistinguishability.
3. If the inequalities are satisfied for specifical exponential-size quantum circuit family $\{C_n\}$ it results the definitions of physical indistinguishability, here the size is determined by the protocol.

The physical security we presented here means that even it may be not information-theoretical secure, the way to attack is unable to realize limited to the objective physical conditions.

3.5. The necessary and sufficient condition for information-theoretic indistinguishability

Here we present the sufficient and necessary condition of the information-theoretic indistinguishability for quantum private-key encryption scheme as follow:

Theorem 1. *For every plaintexts x and y and key k, let the density operators of cipher states $\sum_k p_k E_k(x)$ and $\sum_k p_k E_k(y)$ are ρ_x and ρ_y, respectively. A quantum private-key encryption scheme is said to be information-theoretically indistinguishable if for every positive polynomial $p(\cdot)$ and every sufficiently large n,*

$$D(\rho_x, \rho_y) < \frac{1}{p(n)}. \tag{13}$$

Proof. For every quantum circuit family $\{C_n\}$,

$$\begin{aligned}
& \Pr[C_n(E_{G(1^n)}(x)) = 1] \\
= \; & \sum_k p_k \cdot \Pr[C_n(E_k(x) \otimes \sigma) = 1] \\
= \; & \Pr[C_n(\sum_k p_k E_k(x) \otimes \sigma) = 1] \\
= \; & \Pr[C_n(\rho_x \otimes \sigma) = 1], \qquad (14)
\end{aligned}$$

where σ is the density operator of service bits of C_n.

Similarly,

$$\Pr[C_n(E_{G(1^n)}(y)) = 1] = \Pr[C_n(\rho_y \otimes \sigma) = 1]. \tag{15}$$

Any quantum circuit family C_n built for distinguishing two density operators corresponds to a set of positive operator-values measure (POVM) $\{E_m\}$. Define $p_m = \mathrm{Tr}(C_n(\rho_x \otimes \sigma)E_m)$, $q_m = \mathrm{Tr}(C_n(\rho_y \otimes \sigma)E_m)$ the probabilities of measurement outcomes labeled by m. In this case, we have:

$$\begin{aligned}
& \Big| \Pr[C_n(\rho_x \otimes \sigma) = 1] - \Pr[C_n(\rho_y \otimes \sigma) = 1] \Big| \\
\le \; & \max_{\{E_m\}} \frac{1}{2} \sum_m |\mathrm{Tr}[E_m(C_n(\rho_x \otimes \sigma) - C_n(\rho_y \otimes \sigma))] \\
= \; & \max_{\{E_m\}} D(p_m, q_m). \qquad (16)
\end{aligned}$$

The last formula is equal to

$$D(C_n(\rho_x \otimes \sigma), C_n(\rho_y \otimes \sigma)) \le D(\rho_x \otimes \sigma, \rho_y \otimes \sigma) = D(\rho_x, \rho_y) < \frac{1}{p(n)}. \tag{17}$$

Hence, according to the Definition 7, the theorem follows. □

For quantum public-key encryption scheme, we also have a theorem:

Theorem 2. *For every plaintexts x and y and public-key k, let the density operators of cipher states $\sum_k p_k E_k(x)$ and $\sum_k p_k E_k(y)$ are ρ_x and ρ_y, respectively. A quantum private-key encryption scheme is said to be information-theoretically indistinguishable if for every positive polynomial $p(\cdot)$ and every sufficiently large n,*

$$D(\rho_x, \rho_y) < \frac{1}{p(n)}. \tag{18}$$

the proof for quantum public-key encryption scheme is similar to the above.

4. Semantic security for quantum encryption scheme

The semantic security for quantum encryption scheme means that whatever can be efficiently computed from the ciphertext can be efficiently computed when given only the length of plaintext. For quantum private-key encryption scheme it turns out as:

Definition 9. *A quantum private-key encryption scheme is semantically secure if for every quantum algorithm A there exist a quantum algorithm A', such that for for every probability ensemble $\{X_n\}_{n\in\mathbb{N}}$, with $|X_n| \le poly(n)$, every quantum bounded functions f, h, positive polynomial $p(\cdot)$, all sufficiently large n:*

$$\begin{aligned} & \Pr[A(1^n, E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) \\ = \;& f(1^n, X_n)] < \Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) \\ = \;& f(1^n, X_n)] + \frac{1}{p(n)}. \end{aligned} \tag{19}$$

where the encryption algorithm E should be a quantum algorithm, and both algorithms and functions are output 0 or 1.

Note that here the probability function Pr include more parts than that within classical definitions, besides the probability distribution of G, X_n, A, A', here as the quantum algorithms and functions are both output classical information, the function Pr should include the probability of collapse.

Similarly we can get the definition for quantum public-key encryption scheme:

Definition 10. *A quantum public-key encryption scheme, (G, E, D), is said to be semantically secure if for every quantum algorithm A there exists a quantum algorithm A' such that for every $\{X_n\}_{n\in\mathbb{N}}, f(\cdot), h(\cdot)p(\cdot)$ and n as in Definition 9,*

$$\begin{aligned} & \Pr[A(1^n, G_1(1^n), E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\ < \;& \Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) \\ = \;& f(1^n, X_n) + \frac{1}{p(n)}. \end{aligned} \tag{20}$$

where the encryption algorithm E should be a quantum algorithm, and both algorithms and functions are output 0 or 1.

As aforementioned, the semantic security can also be classified by three different conditions:

1. As defined above, we get the definitions of information-theoretic semantic security.
2. If the inequalities are satisfied while A and A' are bounded with polynomial-time, it results the definitions of computational semantic security.
3. If the inequalities are satisfied while A and A' are bounded with specifical exponential-time, it results the definitions of physical semantic security, here the size is determined by the protocol.

5. Equivalence of the security definitions

Firstly, we state and prove the following theorem for quantum private-key encryption scheme with computational security. The similar results hold for quantum public-key encryption schemes and for quantum private-key encryption scheme with information-theoretic security.

Theorem 3. *A quantum private-key encryption scheme is semantically secure if and only if it is indistinguishable.*

Proof.

1. "indistinguishability" implies "semantic security".
   Firstly, As the scheme is indistinguishable, for every $C_n, p(\cdot), x, n$ as in Def.7 and $y = 1^{|x|}$, we can get the following inequality:

$$\left|\Pr[C_n(E_{G(1^n)}(x)) = 1] - \Pr[C_n(E_{G(1^n)}(1^{|x|})) = 1]\right| < \frac{1}{p(n)}, \qquad (21)$$

   Then we construct the quantum algorithm A' as follow: The quantum algorithm A' performs essentially while replace the input X_n of algorithm A with $1^{|X_n|}$.
   To simplify the notations, let $h_n(x) \doteq h(1^n, x)$, $f_n(x) \doteq f(1^n, x)$, $A_n(x) \doteq A(1^n, x)$ and omit $1^{|X_n|}$ from the inputs given to A, then

using the construction of A' we get:

$$\begin{aligned}
& \Pr[A(1^n, E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\
= \ & \Pr[A_n(E_{G_1(1^n)}(X_n), h_n(X_n)) = f_n(X_n)]; \\
& \Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\
= \ & \Pr[A_n(E_{G_1(1^n)}(1^{|X_n|}), h_n(X_n)) = f_n(X_n)];
\end{aligned} \tag{22}$$

For every string $x_n \in \{X_n\}$, the values $f_n(x_n), h_n(x_n)$ are fixed, then we construct a quantum circuit C_n as follow: on input x_n, the circuit C_n invokes $A_n(E_{G_1(1^n)}(x_n), h_n(x_n))$ and outputs 1 while A_n outputs $f_n(x_n)$, otherwise, C_n outputs 0. This circuit is indeed of polynomial size because $f_n(x_n)$ and $g_n(x_n)$ are polynomial length and A is a polynomial time quantum algorithm.
Thus we can get:

$$\Pr[C_n(E_{G(1^n)}(x)) = 1] = \Pr[A_n(E_{G_1(1^n)}(X_n), h_n(X_n)) = f_n(X_n)]; \tag{23}$$

Proof by contradiction, if the scheme is not semantically secure, then for every A'

$$\begin{aligned}
& \Pr[A(1^n, E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\
> \ & \Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) \\
= \ & f(1^n, X_n)] + \frac{1}{p(n)},
\end{aligned} \tag{24}$$

which is equivalent to that:

$$\Pr[C_n(E_{G(1^n)}(x)) = 1] - \Pr[C_n(E_{G(1^n)}(1^{|x|})) = 1] > \frac{1}{p(n)}, \tag{25}$$

this contradicts InEq.(26), so the sufficiency follows. □

2. "semantic security" implies "indistinguishability".
Also proof by contradiction, if the scheme is not indistinguishable, we can assume that there exists a polynomial $p(\cdot)$ and a polynomial-size circuit family $\{C_n\}$, such that for infinitely many n's there exist $x_n, y_n \in \{0,1\}^{poly(n)}$ so that:

$$\Big|\Pr[C_n(E_{G(1^n)}(x_n)) = 1] - \Pr[C_n(E_{G(1^n)}(y_n)) = 1]\Big| > \frac{1}{p(n)}, \tag{26}$$

Then we define X_n is uniformly distributed over $\{x_n, y_n\}$, define $f(1^n, X_n) = 1$ while $X_n = x_n$ and equals 0 while $X_n = y_n$ with both probability 1/2, and define $h(1^n, X_n)$ equals the description of the circuit C_n while it reveals no information on the value of X_n.
Here we present a polynomial-time quantum algorithm A that, it recovers $C_n = h(1^n, X_n)$, takes $E_{G(1^n)}(x_n)$ as input, and outputs what C_n outputs.
Thus we can get:

$$\begin{aligned} & \Pr[A(1^n, E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \\ = & \frac{1}{2} \cdot \Pr[A(1^n, E_{G_1(1^n)}(x_n), 1^{|x_n|}, C_n) = 1] \\ & + \frac{1}{2} \cdot \Pr[A(1^n, E_{G_1(1^n)}(y_n), 1^{|y_n|}, C_n) = 0] \\ > & \frac{1}{2} + \frac{1}{2p(n)} \end{aligned} \tag{27}$$

In contrast, while the input values $1^n, 1^{|X_n|}$ and $h(1^n, X_n)$ are independent of the random variable $f(1^n, X_n)$, A' can not output $f(1^n, X_n)$ with success probability above 1/2, so we get:

$$\Pr[A'(1^n, 1^{|X_n|}, h(1^n, X_n)) = f(1^n, X_n)] \leq \frac{1}{2}. \tag{28}$$

Combining InEqs.(27),(28), we reach a contradiction to the hypothesis that the scheme is semantically secure. Thus the necessity follows. □
As both sides of the theorem are proved, the theorem is proven. ■

6. Conclusions

In this paper we suggest definitions of indistinguishability and sematic security for quantum encryption schemes with information-theoretic security, physical security and commotional security. We show that a necessary and sufficient condition leads to information-theoretic indistinguishability, which is useful for proving this security. We proved the equivalence between the indistinguishability and semantic security with computational security of quantum encryption schemes, the other equivalence is also hold with similar proof.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Grant No. 61173157), Strategy Pilot Project of Chinese Academy of Sciences (Grant No. Sub-project XD06010702), and IIEs Cryptography Research Project.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin-tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing , pp. 175, 1984.

[2] L. Yang, "Quantum public-key cryptosystem based on classical NP-complete problem," e-print arXiv: quant-ph/0310076 , 2003.

[3] G. M. Nikolopoulos, "Applications of single-qubit rotations in quantum public-key cryptography," Phys. Rev. A 77, pp. 032348, 2008.

[4] F. Gao, Q. Y. Wen, S. J. Qin, and F. C. Zhu, "Quantum asymmetric cryptography with symmetric keys," Science in China Series G: Physics Mechanics and Astronomy 52, pp. 1925, 2008.

[5] L. Yang, M. Liang, B. Li, L. Hu, and D. G. Feng, "Quantum public-key cryptosystems based on induced trapdoor one-way transformations," e-print arXiv: 1012.5249 , 2010.

[6] P. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," Phys. Rev. A 67(4), pp. 42317, 2003.

[7] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channel," Proc. 41st FOCS , pp. 547, 2000.

[8] A. Ambainis and A. Smith, "Small pseudo-random families of matrices: Derandomizing approximate quantum encryption," Proc. RANDOM, LNCS 3122, Berlin-Heidelberg-NewYork: Springer , pp. 249, 2004.

[9] J. Y. Pan and L. Yang, "Quantum public-key encryption with information theoretic security," e-print arXiv:1006.0354 , 2010.

[10] C. Xiang and L. Yang, "Quantum unicity distance," Proc. SPIE 8440, pp. 84400T, 2012.

[11] L. Yang, C. Xiang, and B. Li, "Qubit-string-based bit commitment protocols with physical security," e-print arXiv: 1011.5099 , 2010.

[12] S. Goldwasser and S. Micali, "Probabilistic encryption," Special issue of Journal of Computer and Systems Sciences 28(2), pp. 270, 1984.

[13] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," Proceedings of the fourteenth annual ACM symposium on Theory of computing , pp. 365, 1982.

[14] O. Goldreich, "Foudations of cryptography: Basic applications," Cambridge University Press , 2001.